UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF NORTH CAROLINA

GENEVIEVE JONES, ELAINE QUITTKAT, JAMIE PERKINS and LYNN CAVERLY, on behalf of all others similarly situated, Plaintiffs, v. EASTERN RADIOLOGISTS, INC. Defendant.	**CASE NO.:** 4:24-cv-49 **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiffs Genevieve Jones, Elaine Quittkat, Jamie Perkins and Lynn Caverly, individually and on behalf of all others similarly situated, by and through their undersigned counsel, bring this Class Action Complaint against Eastern Radiologists, Inc. (herein "Eastern Radiologists" or "Defendant"). Plaintiffs allege the following upon information and belief based on the investigation of counsel, except as to those allegations that specifically pertain to Plaintiffs, which are alleged upon personal knowledge.

INTRODUCTION

1. Plaintiffs and the proposed Class Members bring this class action lawsuit on behalf of all persons who entrusted Defendant with personally identifiable information ("PII")[1] and protected health information ("PHI") that was subsequently exposed in a data breach, which Defendant publicly disclosed on February 29, 2024 (the "Data Breach" or the "Breach").[2]

[1] Personally identifiable information generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 C.F.R. § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual.

[2] *Breach Portal: Cases Currently Under Investigation*, U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last visited March 14, 2024); *see also Eastern Radiologists, Notice of Security Incident*, https://www.easternrad.com/notice-of-security-incident/ (last visited March 14, 2024).

2. Plaintiffs' claims arise from Defendant's failure to properly secure and safeguard Plaintiffs' PII and PHI, which were entrusted to Defendant for the purpose of obtaining medical care, and the accompanying responsibility to securely store and transfer that information that Defendant accepted by accepting Plaintiffs' PII and PHI. Over 880,000 patients' information was affected by the Data Breach, including, but not limited to, patient names, Social Security numbers, medical record numbers, diagnostic testing results, names of treatment facilities, and names of healthcare providers.[3]

3. Defendant is a healthcare services provider based out of Greenville, North Carolina. Defendant provides a wide range of imaging services, including CT scans, MRIs, radiography, fluoroscopy, and ultrasound.[4] Eastern Radiologists also offers migraine treatment, oncologic interventions, and varicose vein treatment.[5] Defendant employs more than 116 people and generates approximately $18 million in annual revenue.[6]

4. In the ordinary course of business, Defendant collects, stores and shares patients' PII and PHI.

5. Starting on or around November 20, 2023, and continuing through November 24, 2023, information related to Defendant's patients was impacted by a cyberattack on Defendant's IT systems.[7]

6. On November 24, 2023, Defendant identified suspicious activity on their network and began an investigation.[8]

---

[3] *Id.*
[4] *See* Eastern Diagnostics, Inc., *OUR PRACTICE, History & Message*, https://www.easternrad.com/history-message/ (last visited March 14, 2024).
[5] *Id.*
[6] *See* JD SUPRA, *Eastern Radiologists Files Notice of Data Breach Affecting over 886,000 Patients*, https://www.jdsupra.com/legalnews/eastern-radiologists-files-notice-of-9036169/ (last visited March 14, 2024).
[7] *Eastern Radiologists, Notice of Security Incident*, https://www.easternrad.com/notice-of-security-incident/ (last visited March 14, 2024).
[8] *Id.*

7. On January 26, 2024, upon completion of their investigation two months after it began, Defendant determined that files containing patients' information were accessed and/or copied in the breach. [9] These files included patients' name, contact information, Social Security number, insurance information, exam and/or procedure information, referring physician, diagnosis information and/or imaging results.[10]

8. On February 29, 2024, a month after completing its investigation, Defendant filed a notice of data breach with the U.S. Department of Health and Human Services Office for Civil Rights, indicating more than 880,000 patients were impacted by the data breach.[11]

9. Thereafter, on March 4, 2024, Defendant began notifying all patients whose information was impacted by the data breach.[12] Such notice ultimately came three months after discovering the Data Breach.

10. Defendant had numerous statutory, regulatory, contractual, and common law duties and obligations, including those based on its affirmative representations to Plaintiffs and the Class, to keep their PII and PHI confidential, safe, secure, and protected from unauthorized disclosure or access.

11. Plaintiffs' claims arise from Defendant's failure to safeguard PII and PHI provided by and belonging to its patients and failure to provide timely notice of the Data Breach.

12. Defendant failed to take precautions designed to keep its patients' PII and PHI.

13. Defendant owed Plaintiffs and Class Members a non-delegable duty to take all reasonable and necessary measures to keep the PII and PHI it collected safe and secure from

[9] *Id.*
[10] *Id.*
[11] *Breach Portal: Cases Currently Under Investigation*, U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last visited March 14, 2024).
[12] *Eastern Radiologists, Notice of Security Incident*, https://www.easternrad.com/notice-of-security-incident/ (last visited March 14, 2024).

unauthorized access. Defendant solicited, collected, used, and derived a benefit from the PII and PHI, yet breached its duty by failing to implement or maintain adequate security practices.

14. Defendant admits that its patients' PII and PHI was accessed by unauthorized individuals, though they have provided little information on how the data breach occurred.

15. The sensitive nature of the data exposed through the Data Breach, including Social Security numbers, medical records, claims history and health data highlights that Plaintiffs and Class members have suffered irreparable harm. Plaintiffs and Class members have lost the ability to control their private information and are exposed to continued attempts of identity theft.

16. Defendant inexcusably delayed disclosing and providing notice of the Data Breach to its patients. Defendant knew its patients' PII and PHI were compromised in the Data Breach on January 26, 2023, yet did not send notices to impacted patients until March 4, 2024.13

17. Defendant, despite having the financial wherewithal and personnel necessary to prevent the Data Breach, nevertheless failed to use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted and unredacted information it maintained for Plaintiffs and members of the Class, causing the exposure of Plaintiffs' and Class Members' PII and PHI.

18. As a result of Defendant's inadequate digital security and notice process, Plaintiffs' and Class members' PII and PHI were exposed to criminals. Plaintiffs and the Class have suffered, and will continue to suffer, injuries including: financial losses caused by misuse of PII and PHI; the loss or diminished value of their PII and PHI as a result of the Data Breach; lost time associated with detecting and preventing identity theft; and theft of personal and financial information.

[13] *Id.*

19. Plaintiffs bring this action on behalf of all persons whose PII and PHI were compromised as a result of Defendant's failure to: (i) adequately protect the PII and PHI of Plaintiffs and members of the Class; (ii) warn Plaintiffs and members of the Class of Defendant's inadequate information security practices; (iii) effectively secure hardware containing protected PII and PHI using reasonable and adequate security procedures free of vulnerabilities and incidents; and (iv) timely notify Plaintiffs and members of the Class of the Data Breach. Defendant's conduct amounts at least to negligence and violates federal and state statutes.

20. Plaintiffs bring this action individually and on behalf of a Nationwide Class of similarly situated individuals against Defendant for: negligence; negligence per se; breach of implied contract; unjust enrichment; and invasion of privacy. Plaintiffs also bring this action on behalf of a North Carolina subclass for violations of the North Carolina Unfair Trade Practices Act, N.C. Gen. Stat. Ann. §§ 75-1.1., et seq., and North Carolina Identity Theft Protection Act, N.C. Gen. Stat. Ann. §§ 75-60., et seq.

21. Plaintiffs seek to remedy these harms and prevent any future data compromise on behalf of themselves and all similarly situated persons whose personal data was compromised and stolen as a result of the Data Breach and who remain at risk due to Defendant's inadequate data security practices.

JURISDICTION AND VENUE

22. This Court has jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. At least one member of the Class defined below is a citizen of a different state than Defendant, and there are more than 100 putative Class members. This Court also has supplemental jurisdiction pursuant to 28 U.S.C. § 1367(a) because all claims alleged herein form part of the same case or controversy.

23. This Court has personal jurisdiction over Defendant because Defendant maintains and operates its headquarters in this District.

24. Venue is proper in these District under 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to the claims occurred in this District. Additionally, venue is proper because Plaintiff Jones is a resident of Greene County, Plaintiff Quittkat is a resident of Lenoir County, Plaintiff Perkins is a resident of Washington County and Plaintiff Caverly is a resident of Pitt County, all within this District.

PARTIES

25. Plaintiff Genevieve Jones is a citizen of North Carolina and resides in Snow Hill located in Greene County. Plaintiff Jones received a notice of Data Breach letter – dated March 4, 2024 –informing her that her PII and PHI were compromised in the Data Breach. As a consequence of the Data Breach, Ms. Jones has been forced to, and will continue to, invest significant time monitoring her accounts to detect and reduce the consequences of likely identity fraud. Plaintiff Jones is subject to substantial and imminent risk of future harm.

26. Plaintiff Elaine Quittkat is a citizen of North Carolina and resides in Kinston located in Lenoir County. Plaintiff Quittkat received a notice of data breach letter – dated March 4, 2024 – informing her that her PII and PHI were compromised in the Data Breach. As a consequence of the Data Breach, Ms. Quittkat has been forced to, and will continue to, invest significant time monitoring her accounts to detect and reduce the consequences of likely identity fraud. Plaintiff Quittkat is subject to substantial and imminent risk of future harm.

27. Plaintiff Jamie Perkins is a citizen of North Carolina and resides in Plymouth located in Washington County. Plaintiff Perkins received a notice of Data Breach letter – dated March 4, 2024 –informing her that her PII and PHI were compromised in the Data Breach. As a consequence of the Data Breach, Ms. Perkins has been impacted by an increase in telemarketing

and spam calls. Ms. Perkins has been forced to, and will continue to, invest significant time monitoring her accounts to detect and reduce the consequences of likely identity fraud. Plaintiff Perkins is subject to substantial and imminent risk of future harm.

28. Plaintiff Lynn Caverly is a citizen of North Carolina and resides in Greenville located in Pitt County. Plaintiff Caverly received a notice of data breach letter – dated March 4, 2024 – informing her that her PII and PHI were compromised in the Data Breach. As a consequence of the Data Breach, Ms. Caverly has been forced to, and will continue to, invest significant time monitoring her accounts to detect and reduce the consequences of likely identity fraud. Plaintiff Caverly is subject to substantial and imminent risk of future harm.

29. Defendant Eastern Radiologists, Inc. is a healthcare services provider based out of Greenville, North Carolina. Defendant provides a wide range of imaging services, including CT scans, MRIs, radiography, fluoroscopy, and ultrasound.[14] Eastern Radiologists also offers migraine treatment, oncologic interventions, and varicose vein treatment.[15] Defendant employs more than 116 people and generates approximately $18 million in annual revenue.[16]

30. Defendant collected and continues to collect and transmit the PII and PHI of patients throughout their usual course of business operations. By obtaining, collecting, using, and deriving benefit from Plaintiffs' and Class's PII and PHI, Defendant assumed legal and equitable duties to those persons, and knew or should have known that it was responsible for protecting Plaintiffs' and Class's PII and PHI from unauthorized disclosure and/or criminal cyber activity.

[14] *See* Eastern Diagnostics, Inc., *OUR PRACTICE, History & Message*, https://www.easternrad.com/history-message/ (last visited March 14, 2024).
[15] *Id.*
[16] *See* JD SUPRA, *Eastern Radiologists Files Notice of Data Breach Affecting over 886,000 Patients*, https://www.jdsupra.com/legalnews/eastern-radiologists-files-notice-of-9036169/ (last visited March 14, 2024).

FACTUAL BACKGROUND

A. Background on Defendant

31. Defendant is a healthcare services provider that offers a wide range of imaging services, including CT scans, MRIs, radiography, fluoroscopy, and ultrasound, as well as migraine treatment, oncologic interventions, and varicose vein treatment.

32. In the ordinary course of their business practices, Defendant obtains, stores, maintains, uses, and transmits individuals' PII and PHI including but not limited to information such as: full names; Social Security numbers; medical record numbers, diagnostic testing results, names of treatment facilities, and names of healthcare providers.

33. Upon information and belief, Defendant made promises and representations to its patients, including Plaintiffs and Class members, that the PII and PHI collected from them would be kept safe, confidential, that the privacy of that information would be maintained, and that Defendant would delete any sensitive information after it was no longer required to maintain it.

34. Plaintiffs and Class members had a reasonable expectation that Defendant would keep their information confidential and secure from unauthorized access.

35. As a result of collecting and storing the PII and PHI of Plaintiffs and members of the Class for its own financial benefit, Defendant had a continuous duty to adopt and employ reasonable measures to protect Plaintiffs and the Class Members' PII and PHI from disclosure to third parties.

B. The Data Breach

36. Starting on or around November 20, 2023, and continuing through November 24, 2023, an unauthorized party gained access to Defendant's IT systems.[17]

[17] *Eastern Radiologists, Notice of Security Incident*, https://www.easternrad.com/notice-of-security-incident/ (last visited March 14, 2024).

37. On November 24, 2023, Defendant identified the security threat and began investigation.[18] Defendant notified law enforcement, began working with leading cybersecurity experts to investigate the incident.[19]

38. On January 26, 2024, upon completion of their investigation, Defendant determined that their patients' information was compromised in the breach, including patients' name, contact information, Social Security number, insurance information, exam and/or procedure information, referring physician, diagnosis information and/or imaging results.[20]

39. On February 29, 2024, Defendant filed a notice of data breach with the U.S. Department of Health and Human Services Office for Civil Rights, indicating more than 880,000 patients were impacted by the data breach.[21]

40. Thereafter, on March 4, 2024, Defendant began notifying all patients whose information was impacted by the data breach.[22]

41. Defendant has admitted there was unauthorized access to the PII and PHI of Plaintiffs and Class Members.

42. Individuals affected by the Data Breach are, and remain, at risk that their data will be sold or listed on the dark web and, ultimately, illegally used in the future.

C. Defendant's Failure to Prevent, Identify and Timely Report the Data Breach

43. Defendant admits that unauthorized third persons accessed from its network systems sensitive information about its current and former customers.

---

[18] *Id.*
[19] *Id.*
[20] *Id.*
[21] *Breach Portal: Cases Currently Under Investigation*, U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last visited March 14, 2024).
[22] *Eastern Radiologists, Notice of Security Incident*, https://www.easternrad.com/notice-of-security-incident/ (last visited March 14, 2024).

44. Defendant failed to take adequate measures to protect its computer systems against unauthorized access.

45. Defendant was aware of the importance of protecting the PHI and PII that it maintains. The PII and PHI that Defendant allowed to be exposed in the Data Breach is the type of private information that Defendant knew or should have known would be the target of cyberattacks.

46. Despite its own knowledge of the inherent risks of cyberattacks, and notwithstanding the FTC's data security principles and practices,[23] Defendant failed to disclose that its systems and security practices were inadequate to reasonably safeguard its customers' sensitive personal information.

47. The FTC directs businesses to use an intrusion detection system to expose a breach as soon as it occurs, monitor activity for attempted hacks, and have an immediate response plan if a breach occurs.[24] Immediate notification of a Data Breach is critical so that those impacted can take measures to protect themselves.

48. Despite this guidance, Defendant delayed the notification of the Data Breach. Defendant completed their investigation of the Data Berach on January 26, 2024, yet did not file a public disclosure until February 29, 2024, and did not begin informing impacted patients until March 4, 2024.

D. The Harm Caused by the Data Breach Now and Going Forward.

49. Victims of data breaches are susceptible to becoming victims of identity theft.

[23] *Protecting Personal Information: A Guide for Business*, FEDERAL TRADE COMMISSION (Oct. 2016), https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business (last visited March 14, 2024).
[24] *Id.*

50. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority," 17 C.F.R. § 248.201(9), and when "identity thieves have your personal information, they can drain your bank account, run up charges on your credit cards, open new utility accounts, or get medical treatment on your health insurance."[25]

51. The type of data that was accessed and compromised here – including Social Security numbers – can be used to perpetrate fraud and identity theft. Social Security numbers are widely regarded as the most sensitive information hackers can access. Social Security numbers and dates of birth together constitute high risk data.

52. Plaintiffs and Class Members face a substantial risk of identity theft given that their Social Security numbers, addresses, and/or dates of birth were compromised. Once a Social Security number is stolen, it can be used to identify victims and target them in fraudulent schemes and identity theft.

53. Stolen PII and PHI are often trafficked on the "dark web," a heavily encrypted part of the Internet that is not accessible via traditional search engines. Law enforcement has difficulty policing the "dark web" due to this encryption, which allows users and criminals to conceal identities and online activity.

54. When malicious actors infiltrate companies and copy and exfiltrate the PII and PHI that those companies store, that stolen information often ends up on the dark web because the malicious actors buy and sell that information for profit.[26]

[25] *Prevention and Preparedness*, NEW YORK STATE POLICE, https://troopers.ny.gov/prevention-and-preparedness (last visited March 14 2024).
[26] *Shining a Light on the Dark Web with Identity Monitoring*, IDENTITYFORCE, Dec. 28, 2020, *available at:* https://www.identityforce.com/blog/shining-light-dark-web-identity-monitoring (last visited March 14, 2024).

55. For example, when the U.S. Department of Justice announced its seizure of AlphaBay in 2017, AlphaBay had more than 350,000 listings, many of which concerned stolen or fraudulent documents that could be used to assume another person's identity. Other marketplaces, similar to the now-defunct AlphaBay, "are awash with [PII] belonging to victims from countries all over the world. One of the key challenges of protecting PII online is its pervasiveness. As data breaches in the news continue to show, PII about employees, customers and the public is housed in all kinds of organizations, and the increasing digital transformation of today's businesses only broadens the number of potential sources for hackers to target."[27]

56. PII and PHI remain of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[28] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[29]

57. A compromised or stolen Social Security number cannot be addressed as simply as, perhaps, a stolen credit card. An individual cannot obtain a new Social Security number without significant work. Preventive action to defend against the possibility of misuse of a Social Security number is not permitted; rather, an individual must show evidence of actual, ongoing fraud activity to obtain a new number. Even then, however, obtaining a new Social Security number may not suffice. According to Julie Ferguson of the Identity Theft Resource Center, "The

[27] *Stolen PII & Ramifications: Identity Theft and Fraud on the Dark Web*, ARMOR, April 3, 2018, *available at:* https://res.armor.com/resources/blog/stolen-pii-ramifications-identity-theft-fraud-dark-web/ (last visited March 14, 2024).
[28] *Id.*
[29] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), available at: https://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last visited March 14, 2024).

credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[30]

58. The PII and PHI compromised in the Data Breach demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained: "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10 times on the black market."[31]

59. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses in 2019, resulting in more than $3.5 billion in losses to individuals and business victims.[32]

60. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good."[33]

61. As a result of the Data Breach, the PII and PHI of Plaintiffs and Class members have been exposed to criminals for misuse. The injuries suffered by Plaintiffs and Class members, or likely to be suffered thereby as a direct result of Defendant's Data Breach, include:

a. unauthorized use of their PII and PHI;

b. theft of their personal and financial information;

c. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

d. damages arising from the inability to use their PII and PHI;

e. Improper disclosure of their PII and PHI;

---

[30] *Id.*

[31] *Experts advise compliance not same as security*, RELIAS MEDIA https://www.reliasmedia.com/articles/134827-experts-advise-compliance-not-same-as-security (last visited March 14, 2024).

[32] *2019 Internet Crime Report Released*, FBI, https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120#:~:text=IC3%20received%20467%2C361%20complaints%20in,%2Ddelivery%20scams%2C%20and%20extortion. (last visited March 14, 2024).

[33] *Id.*

f. loss of privacy, and embarrassment;

g. trespass and damage their personal property, including PII and PHI;

h. the imminent and certainly impending risk of having their confidential medical information used against them by spam callers and/or hackers targeting them with phishing schemes to defraud them;

i. costs associated with time spent and the loss of productivity or the enjoyment of one's life from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach, including finding fraudulent charges, purchasing credit monitoring and identity theft protection services, and the stress, nuisance, and annoyance of dealing with all issues resulting from the Data Breach;

j. the imminent and certainly impending injury flowing from potential fraud and identify theft posed by their PII and PHI being placed in the hands of criminals and already misused via the sale of Plaintiffs' and Class members' information on the Internet black market; and

k. damages to and diminution in value of their PII entrusted to Defendant for the sole purpose of obtaining medical services from Defendant, and the loss of Plaintiffs' and Class members' privacy.

l. In addition to a remedy for economic harm, Plaintiffs and Class members maintain an interest in ensuring that their PII and PHI is secure, remains secure, and is not subject to further misappropriation and theft.

62. Defendant disregarded the rights of Plaintiffs and Class members by (i) intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure that its network servers were protected against unauthorized intrusions; (ii)

failing to disclose that it did not have adequately robust security protocols and training practices in place to adequately safeguard Plaintiffs' and Class members' PII and PHI; (iii) failing to take standard and reasonably available steps to prevent the Data Breach; (iv) concealing the existence and extent of the Data Breach for an unreasonable duration of time; and (v) failing to provide Plaintiffs and Class members prompt and accurate notice of the Data Breach.

63. The actual and adverse effects to Plaintiffs and Class members, including the imminent, immediate, and continuing increased risk of harm for identity theft, identity fraud, and/or medical fraud directly and/or proximately caused by Defendant's wrongful actions and/or inaction. The resulting Data Breach requires Plaintiffs and Class members to take affirmative acts to recover their peace of mind and personal security including, without limitation: purchasing credit reporting services; purchasing credit monitoring and/or internet monitoring services; frequently obtaining, purchasing, and reviewing credit reports, bank statements, and other similar information; instituting and/or removing credit freezes; and modifying and/or closing financial accounts, for which there is a financial and temporal cost. Plaintiffs and other Class members have suffered, and will continue to suffer, such damages for the foreseeable future.

CLASS ACTION ALLEGATIONS

64. Plaintiffs bring this action pursuant to Rule 23 of the Federal Rules of Civil Procedure, individually and on behalf of the following Classes:

> All persons in the United States whose personal information was compromised in the Data Breach publicly announced by Defendant in February 2024 (the "Class").
>
> All persons in North Carolina whose personal information was compromised in the Data Breach publicly announced by Defendant in February 2024 (the "North Carolina Subclass").

65. Specifically excluded from the Class is the Defendant, its officers, directors, agents, trustees, parents, children, corporations, trusts, representatives, employees, principals, servants, partners, joint venturers, or entities controlled by Defendant, and their heirs, successors,

assigns, or other persons or entities related to or affiliated with Defendant and/or its officers and/or directors, the judge assigned to this action, and any member of the judge's immediate family.

66. Plaintiffs reserve the right to amend the Class definitions above if further investigation and/or discovery reveals that the Class should be expanded, narrowed, divided into subclasses, or otherwise modified in any way.

67. This action may be certified as a class action under Federal Rule of Civil Procedure 23 because it satisfies the numerosity, commonality, typicality, adequacy, and superiority requirements therein.

68. Numerosity (Rule 23(a)(1)): The Class is so numerous that joinder of all Class members is impracticable. Although the precise number of such persons is unknown, and the facts are presently within the sole knowledge of Defendant, Plaintiffs estimate that the Class is comprised of millions of Class members. The Class is sufficiently numerous to warrant certification.

69. Typicality of Claims (Rule 23(a)(3)): Plaintiffs' claims are typical of those of other Class Members because they all had their PII compromised as a result of the Data Breach. Plaintiffs are members of the Class, and their claims are typical of the claims of the members of the Class. The harm suffered by Plaintiffs is similar to that suffered by all other Class members that was caused by the same misconduct by Defendant.

70. Adequacy of Representation (Rule 23(a)(4)): Plaintiffs will fairly and adequately represent and protect the interests of the Class. Plaintiffs have no interests antagonistic to, nor in conflict with, the Class. Plaintiffs have retained competent counsel who are experienced in consumer and commercial class action litigation and who will prosecute this action vigorously.

71. Superiority (Rule 23(b)(3)): A class action is superior to other available methods for the fair and efficient adjudication of this controversy. Because the monetary damages suffered

by individual Class members is relatively small, the expense and burden of individual litigation make it impossible for individual Class members to seek redress for the wrongful conduct asserted herein. If Class treatment of these claims is not available, Defendant will likely continue its wrongful conduct, will unjustly retain improperly obtained revenues, or will otherwise escape liability for its wrongdoing as asserted herein.

72. Predominant Common Questions (Rule 23(a)(2)): The claims of all Class members present common questions of law or fact, which predominate over any questions affecting only individual Class members, including:

a. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

b. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

c. Whether Defendant negligently stored of Class Member's PII and PHI;

d. Whether Defendant had a duty to protect and safeguard Plaintiffs' and Class Members' PII and PHI;

e. Whether Defendant negligently responded to the Data Breach by taking months to notify its patients, including Plaintiffs and Class Members;

f. Whether Defendant's conduct violated Plaintiffs' and Class Members' privacy;

g. Whether Defendant took sufficient steps to secure their customers' PII and PHI;

h. Whether Defendant was unjustly enriched;

i. The nature of relief, including damages and equitable relief, to which Plaintiffs and members of the Class are entitled.

73. Information concerning Defendant's policies is available from Defendant's records.

74. Plaintiffs know of no difficulty which will be encountered in the management of this litigation which would preclude their maintenance as a class action.

75. The prosecution of separate actions by individual members of the Class would run the risk of inconsistent or varying adjudications and establish incompatible standards of conduct for Defendant. Prosecution as a class action will eliminate the possibility of repetitious and inefficient litigation.

76. Defendant has acted or refused to act on grounds generally applicable to the Class, thereby making appropriate final injunctive relief or corresponding declaratory relief with respect to the Class as a whole.

77. Given that Defendant has not indicated any changes to its conduct or security measures, monetary damages are insufficient and there is no complete and adequate remedy at law.

CAUSES OF ACTION

COUNT I
NEGLIGENCE
(On Behalf of Plaintiffs and All Class Members)

78. Plaintiffs repeat and re-allege each and every factual allegation contained in paragraphs 1-21 and 31-63 as if fully set forth herein.

79. Plaintiffs bring this claim individually and on behalf of the Class members.

80. Defendant knowingly collected, came into possession of, and maintained Plaintiffs' and Class Members' PII and PHI, and had a duty to exercise reasonable care in

safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties.

81. Defendant had a duty to have procedures in place to detect and prevent the loss or unauthorized dissemination of Plaintiffs' and Class Members' PII and PHI.

82. Defendant had, and continues to have, a duty to timely disclose that Plaintiffs' and Class Members' PII and PHI within its possession was compromised and precisely the type(s) of information that was compromised.

83. Defendant owed a duty of care to Plaintiffs and Class Members to provide data security consistent with industry standards, applicable standards of care from statutory authority like Section 5 of the FTC Act, and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected its customers' PII and PHI.

84. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and its patients. Defendant was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach.

85. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential PII and PHI.

86. Defendant breached these duties by failing to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class members' PII and PHI.

87. The specific negligent acts and omissions committed by Defendant includes, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' PII and PHI;

b. Failing to adequately monitor the security of their networks and systems; and

c. Failing to periodically ensure that their computer systems and networks had plans in place to maintain reasonable data security safeguards.

88. Defendant, through its actions and/or omissions, unlawfully breached its duties to Plaintiffs and Class members by failing to exercise reasonable care in protecting and safeguarding Plaintiffs' and Class Members' PII and PHI within Defendant's possession.

89. Defendant, through its actions and omissions, unlawfully breached its duties to Plaintiffs and Class members by failing to have appropriate procedures in place to detect and prevent dissemination of Plaintiffs' and Class Members' PII and PHI.

90. Defendant, through its actions and/or omissions, unlawfully breached its duty to timely disclose to Plaintiffs and Class Members that the PII and PHI within Defendant's possession had been compromised and precisely the type of information compromised.

91. Defendant breached the duties set forth in 15 U.S.C. § 45, the FTC guidelines, the NIST's Framework for Improving Critical Infrastructure Cybersecurity, and other industry guidelines. In violation of 15 U.S.C. § 45, Defendant failed to implement proper data security procedures to adequately and reasonably protect Plaintiffs' and Class Member's PII and PHI. In violation of the FTC guidelines, *inter alia*, Defendant did not protect the personal customer information it keeps; failed to properly dispose of personal information that was no longer needed; failed to encrypt information stored on computer networks; lacked the requisite understanding of its networks' vulnerabilities; and failed to implement policies to correct security issues.

92. It was foreseeable that Defendant's failure to use reasonable measures to protect Plaintiffs' and Class Members' PII and PHI would result in injury to Plaintiffs and Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches.

93. It was foreseeable that the failure to adequately safeguard Plaintiffs' and Class Members' PII and PHI would result in injuries to Plaintiffs and Class Members.

94. Defendant breach of duties owed to Plaintiffs and Class Members caused Plaintiffs' and Class Members' PII and PHI to be compromised.

95. But for Defendant's negligent conduct and breach of the above-described duties owed to Plaintiffs and Class members, their PII and PHI would not have been compromised.

96. As a result of Defendant's failure to timely notify Plaintiffs and Class Members that their PII and PHI had been compromised, Plaintiffs and Class Members were unable to take the necessary precautions to mitigate damages by preventing future fraud.

97. As a result of Defendant's negligence and breach of duties, Plaintiffs and Class Members are in danger of imminent harm in that their PII and PHI which is still in the possession of third parties, will be used for fraudulent purposes, and Plaintiffs and Class Members have and will suffer damages including: a substantial increase in the likelihood of identity theft; the compromise, publication, and theft of their personal information; loss of time and costs associated with the prevention, detection, and recovery from unauthorized use of their personal information; the continued risk to their personal information; future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the personal information compromised as a result of the Data Breach; and overpayment for the services or products that were received without adequate data security.

COUNT II
NEGLIGENCE PER SE
(On Behalf of Plaintiffs and All Class Members)

98. Plaintiffs repeat and re-allege each and every factual allegation contained in paragraphs 1-21 and 31-63, as if fully set forth herein.

99. Section 5 of the FTC Act, 15 U.S.C. 45, prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by Defendant of failing to use reasonable measures to protect Plaintiffs' and Class members' Private Information. Various FTC publications and orders also form the basis of Defendant's duty.

100. Defendant violated Section 5 of the FTC Act (and similar state statutes) by failing to use reasonable measures to protect Plaintiff's and Class members' Private Information and not complying with industry standards.

101. Defendant's conduct was particularly unreasonable given the nature and amount of Private Information obtained and stored and the foreseeable consequences of a data breach on Defendant's systems.

102. Defendant's violation of Section 5 of the FTC Act (and similar state statutes) constitutes negligence per se.

103. Class members are consumers within the class of persons Section 5 of the FTC Act (and similar state statutes) were intended to protect.

104. Moreover, the harm that has occurred is the type of harm the FTC Act (and similar state statutes) was intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiff and Class members.

105. As a result of Defendant's negligence, Plaintiffs and the other Class members have been harmed and have suffered damages including, but not limited to: damages arising from identity theft and fraud; out-of-pocket expenses associated with procuring identity protection and restoration services; increased risk of future identity theft and fraud, and the costs associated therewith; and time spent monitoring, addressing and correcting the current and future consequences of the Data Breach.

COUNT III
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiffs and All Class Members)

106. Plaintiffs repeat and re-allege each and every factual allegation contained in paragraphs 1-21 and 31-63 as if fully set forth herein.

107. Plaintiffs and the Class provided and entrusted their PII and PHI to Defendant. Plaintiffs and the Class provided their PII and PHI to Defendant as part of Defendant's regular business practices.

108. In so doing, Plaintiffs and the Class entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiffs and the Class if their data had been breached and compromised or stolen, in return for the business services provided by Defendant. Implied in these exchanges was a promise by Defendant to ensure that the sensitive information of Plaintiffs and Class members in its possession was secure.

109. Pursuant to these implied contracts, Defendant obtained Plaintiffs' and Class Members' PII and PHI for Defendant to provide services, for which Defendant is compensated. In exchange, Defendant agreed to, among other things, and Plaintiffs understood that Defendant would: (1) provide services to Plaintiffs and Class members; (2) take reasonable measures to protect the security and confidentiality of Plaintiffs' and Class members' PII and PHI; and (3)

protect Plaintiffs' and Class members' PII and PHI in compliance with federal and state laws and regulations and industry standards.

110. Implied in these exchanges was a promise by Defendant to ensure the PII and PHI of Plaintiffs and Class members in their possession was only used to provide the agreed-upon reasons, and that Defendant would take adequate measures to protect the sensitive information.

111. A material term of this contract is a covenant by Defendant that it would take reasonable efforts to safeguard that information. Defendant breached this covenant by allowing Plaintiffs' and Class members' PII and PHI to be accessed in the Data Breach.

112. Indeed, implicit in the agreement between Defendant and the patients was the obligation that both parties would maintain information confidentially and securely.

113. These exchanges constituted an agreement and meeting of the minds between the parties: Plaintiffs and Class members would provide their PII and PHI in exchange for services by Defendant. These agreements were made by Plaintiffs and Class members as Defendant's customers.

114. When the parties entered into an agreement, mutual assent occurred. Plaintiffs and Class members would not have disclosed their PII and PHI to Defendant but for the prospect of utilizing Defendant's services. Conversely, Defendant presumably would not have taken Plaintiffs' and Class members' PII and PHI if it did not intend to provide Plaintiffs and Class members with its services.

115. Defendant was therefore required to reasonably safeguard and protect the sensitive information of Plaintiffs and Class members from unauthorized disclosure and/or use.

116. Plaintiffs and Class Members accepted Defendant's offer of services and fully performed their obligations under the implied contract with Defendant by providing their PII and PHI directly or indirectly, to Defendant, among other obligations.

117. Plaintiffs and Class Members would not have entrusted PII and PHI to Defendant in the absence of their implied contracts with Defendant and would have instead retained the opportunity to control their PII and PHI.

118. Defendant breached the implied contracts with Plaintiffs and Class members by failing to reasonably safeguard and protect Plaintiffs' and Class Members' PII and PHI.

119. Defendant's failure to implement adequate measures to protect the PII and PHI of Plaintiffs and Class Members violated the purpose of the agreement between the parties.

120. Instead of spending adequate financial resources to safeguard Plaintiffs' and Class Members' PII and PHI, which Plaintiffs and Class Members were required to provide to Defendant, Defendant instead used that money for other purposes, thereby breaching its implied contracts it had with Plaintiffs and Class members.

121. As a proximate and direct result of Defendant's breaches of its implied contracts with Plaintiffs and Class Members, Plaintiffs and the Class Members suffered damages as described in detail above.

COUNT IV
UNJUST ENRICHMENT
(On behalf of Plaintiffs and All Class Members)

122. Plaintiffs repeat and re-allege each and every factual allegation contained in paragraphs 1-21 and 31-63 as if fully set forth herein.

123. Plaintiffs and Class Members conferred a benefit upon Defendant by using Defendant's services.

124. Defendant appreciated or had knowledge of the benefits conferred upon itself by Plaintiffs. Defendant also benefited from the receipt of Plaintiffs' PII and PHI as this was used for Defendant to administer its services to Plaintiffs and the Class.

125. Under principles of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiffs' services and their PII and PHI because Defendant failed to adequately protect their sensitive information. Plaintiffs and the proposed Class would not have provided their sensitive information to Defendant or utilized its services had they known Defendant would not adequately protect their PII and PHI.

126. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiffs all unlawful or inequitable proceeds received by it because of their misconduct and Data Breach.

COUNT V
INVASION OF PRIVACY
(On Behalf of Plaintiff and All Class Members)

127. Plaintiffs repeat and re-allege each and every factual allegation contained in paragraphs 1-21 and 31-63, as if fully set forth herein.

128. Plaintiff and Class Members had a legitimate expectation of privacy to their PII and were entitled to the protection of this information against disclosure to unauthorized third parties.

129. Defendant owed a duty to Plaintiff and Class Members to keep their PII contained as a part thereof, confidential.

130. Defendant failed to protect and released to unknown and unauthorized third parties the PII of Plaintiff and Class Members.

131. Defendant allowed unauthorized and unknown third parties access to and examination of the PII of Plaintiff and Class Members, by way of Defendant's failure to protect the PII.

132. The unauthorized release to, custody of, and examination by unauthorized third parties of the PII of Plaintiff and Class Members is highly offensive to a reasonable person.

133. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiff and Class Members disclosed their PII to Defendant as part of their relationships with Defendant in order to receive services from Defendant, but privately with an intention that the PII would be kept confidential and would be protected from unauthorized disclosure. Plaintiff and Class Members were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

134. The Data Breach at the hands of Defendant constitutes an intentional interference with Plaintiff's and Class Member's interest in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

135. Defendant acted with a knowing state of mind when it permitted the Data Breach to occur because it was with actual knowledge that its information security practices were inadequate and insufficient.

136. Because Defendant acted with this knowing state of mind, it had notice and knew the inadequate and insufficient information security practices would cause injury and harm to Plaintiff and Class Members.

137. As a proximate result of the above acts and omissions of Defendant, the PII of Plaintiff and Class Members was disclosed to third parties without authorization, causing Plaintiff and Class Members to suffer damages.

138. Unless enjoined, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and Class Members in that the PII maintained by Defendant can be viewed, distributed, and used by unauthorized persons for years to come. Plaintiff and Class Members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiff and Class Members.

COUNT VI
NORTH CAROLINA UNFAIR TRADE PRACTICES ACT
N.C. Gen. Stat. Ann. §§ 75-1.1., *et seq.*
(On Behalf of Plaintiffs and North Carolina Subclass)

139. Plaintiffs repeat and re-allege each and every factual allegation contained in paragraphs 1-21 and 31-63 as if fully set forth herein.

140. Plaintiffs Jones, Quittkat, Perkins and Caverly, assert this claim on behalf of the North Carolina Subclass.

141. Defendant advertised, offered, or sold goods or services in North Carolina and engaged in trade or commerce directly or indirectly affecting the people of North Carolina, as defined by N.C. Gen. Stat. Ann. § 75-1.1(b).

142. Defendant engaged in unfair and deceptive acts and practices in or affecting commerce, in violation of N.C. Gen. Stat. Ann. § 75-1.1, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs and North Carolina Subclass members' Private Information, which was a direct and proximate cause of the Defendant's data breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Defendant's data breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and North Carolina Subclass members' Personal Information.

d. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

143. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of consumers' Personal Information.

144. Had Defendant disclosed to Plaintiffs and Class members that its data systems were not secure and, thus, vulnerable to attack, Defendant would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law.

145. Defendant was trusted with sensitive and valuable Private Information regarding millions of consumers, including Plaintiff Miller and the North Carolina Subclass. Plaintiffs and the North Carolina Subclass members acted reasonably in relying on Defendant's misrepresentations and omissions, the truth of which they could not have discovered.

146. Defendant acted intentionally, knowingly, and maliciously to violate North Carolina's Unfair Trade Practices Act, and recklessly disregarded Plaintiffs and North Carolina Subclass members' rights.

147. As a direct and proximate result of Defendant's unfair and deceptive acts and practices, Plaintiffs and North Carolina Subclass members have been harmed and have suffered damages including, but not limited to: damages arising from identity theft and fraud; out-of-pocket expenses associated with procuring identity protection and restoration services; increased risk of future identity theft and fraud, and the costs associated therewith; and time spent monitoring, addressing and correcting the current and future consequences of the Data Breach.

148. Plaintiffs and North Carolina Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages, treble damages, and attorneys' fees and costs.

COUNT VII
NORTH CAROLINA IDENTITY THEFT PROTECTION ACT
N.C. Gen. Stat. Ann. §§ 75-60., *et seq.*
(On Behalf of Plaintiffs and North Carolina Subclass)

149. Plaintiffs repeat and re-allege each and every factual allegation contained in paragraphs 1-31 and 31 and 63 as if fully set forth herein.

150. Defendant is a business that owns or licenses computerized data that includes personal information (for the purpose of this count, "PII"), as defined by N.C. Gen. Stat. § 75-61(1).

151. Plaintiffs and North Carolina Subclass Members are "consumers" as defined by N.C. Gen. Stat. § 75-61(2).

152. Defendant is required to accurately notify Plaintiffs and North Carolina Subclass Members if it discovers a security breach or receives notice of a security breach (where unencrypted and unredacted PII was accessed or acquired by unauthorized persons), without unreasonable delay under N.C. Gen. Stat. § 75-65.

153. Plaintiffs' and North Carolina Subclass Members' PII includes PII as covered under N.C. Gen. Stat. § 75-61(10).

154. Since Defendant discovered a security breach and had notice of a security breach (where unencrypted and unredacted PII was accessed or acquired by unauthorized persons), Defendant had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by N.C. Gen. Stat. § 75-65.

155. By failing to disclose the Data Breach in a timely and accurate manner, Defendant violated N.C. Gen. Stat. § 75-65.

156. A violation of N.C. Gen. Stat. § 75-65 is an unlawful trade practice under N.C. Gen. Stat. Art. 2A § 75-1.1.

157. As a direct and proximate result of Defendant's violations of N.C. Gen. Stat. § 75-65, Plaintiff and North Carolina Subclass Members suffered damages, as described above.

158. Plaintiff and North Carolina Subclass Members seek relief under N.C. Gen. Stat. §§ 75-16 and 16.1, including treble damages and attorneys' fees.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of all others similarly situated, seek judgment against Defendant, as follows:

(a) For an order determining that this action is properly brought as a class action and certifying Plaintiffs as the representatives of the Class and their counsel as Class Counsel;

(b) For an order declaring the Defendant's conduct violates the laws referenced herein;

(c) For an order finding in favor of Plaintiffs and the Class on all counts asserted herein;

(d) For damages in amounts to be determined by the Court and/or jury;

(e) An award of statutory damages or penalties to the extent available;

(f) For pre-judgment interest on all amounts awarded;

(g) For an order of restitution and all other forms of monetary relief; and

(h) Such other and further relief as the Court deems necessary and appropriate.

DEMAND FOR TRIAL BY JURY

Plaintiffs demand a trial by jury of all issues so triable.

Dated: March 20, 2024

/s/David M. Wilkerson
David M. Wilkerson
The Van Winkle Law Firm
1 N. Market Street
Asheville, NC 28801
Phone: (828) 258-2991
Fax: (828) 257-2767
dwilkerson@vwlawfirm.com
NC State Bar No. 35742
Local Civil Rule 83.1(d) Attorney for Plaintiff

Eduard Korsinsky*
Mark S. Reich*
LEVI & KORSINSKY, LLP
33 Whitehall Street, 17th Floor
New York, NY 10004
Telephone: (212) 363-7500
Facsimile: (212) 363-7171
Email: ek@zlk.com
mreich@zlk.com

Counsel for Plaintiffs

**pro hac vice* forthcoming